Objetivo:

El presente documento pretende diseñar una guía de gestión de incidentes que permita manejar adecuadamente los incidentes de seguridad de la información y manejo de evidencia digital en el Instituto Distrital de la Artes - IDARTES.

Alcance:

La guía de gestión de incidentes esté dirigido a los funcionarios, contratistas, proveedores de servicios de TIC, proveedores de servicios y contratistas externos

Fecha de Aprobación	Responsable del Documento	Ubicación
03/07/2018	Área de Tecnología	Página Intranet: http://comunicarte.idartes.gov.co/idartes

HISTÓRICO DE CAMBIOS

Versión	Fecha de Emisión	Cambios realizados
01	03. de Julio 2018	Emisión Inicial

Oficinas Participantes

Subdirección Administrativa y Financiera

Elaboró:	Aprobó:	Validó	Aprobó
Luis Albeiro Cortés Contratista Área de TIC	**Juan Carlos Cubillos P** Profesional Universitario Área de TIC **Liliana Valencia Mejía** Subdirectora Administrativa y Financiera	**Camila Crespo Murillo** Contratista Oficina Asesora de Planeación	**Luis Fernando Mejía Castro** Jefe Oficina Asesora de Planeación

CONTENIDO

LISTA DE FIGURAS

LISTA DE TABLAS

INTRODUCCIÓN

El crecimiento de las redes de comunicaciones, sistemas de información e infraestructuras tecnológicas ha creado un nuevo reto para los técnico e ingenieros de sistemas para la prevención, el control y la respuesta a los incidentes de seguridad.

La correcta gestión de los incidentes de seguridad nos permite afrontarlos de forma eficaz, respondiendo en la medida adecuada, sin embargo, muchos de los incidentes son intencionados y provocan daños de muy distinta índole. Una gestión oportuna de los incidentes, así como de su solución, nos permitirá regresar los servicios a un estado anterior, a la par de una correcta recolección de evidencias digitales con valor probatorio ante un tribunal. Igualmente, muchos incidentes de seguridad están provocados accidentalmente por el personal de TI, que no ha seguido o no ha entendido los procedimientos de administración de cambios, o bien no ha configurado correctamente los dispositivos de seguridad, como pueden ser los firewalls o los sistemas de autenticación

En caso de algún evento o incidente de seguridad que requiera de evidencias digitales para su investigación se debe llevar a cabo una correcta identificación, recolección, análisis y manipulación de datos.

1. OBJETIVO DEL DOCUMENTO

El objetivo es diseñar una guía para gestionar la gestión de incidentes que permita manejar adecuadamente los incidentes de seguridad de la información y manejo de evidencia digital en el Instituto Distrital de la Artes - IDARTES.

2. ALCANCE

La guía de gestión de incidentes esté dirigido a los funcionarios, contratistas, proveedores de servicios de TIC, proveedores de servicios y ciudadanía.

3. METODOLOGÍA

El ciclo de funcionamiento del modelo de operación de gestión de incidentes plantea una serie de actividades para dar cumplimiento con el ciclo de vida de la gestión y respuesta a un incidente de seguridad.

Figura 1. Etapas gestión de incidentes

Fuente: GTC-ISO/ IEC 27035 – Guía Gestión de incidentes – MINTIC

3.1 PREPARACIÓN:

Consiste en eliminar la causa que origina el incidente, en esta etapa incluye tanto la prevención de los ataques como la preparación para responder a cada uno. Para ello es necesario tener en cuenta la matriz de riesgos de SGSI, Copias de seguridad, Controles con los proveedores, políticas de SGSI y constituido el CSIRT (Computer Security Incident Response Team, Equipo de Respuesta ante Incidencias de Seguridad) y plan de contingencias de TI.

Para minimizar la repercusión de los incidentes es conveniente:

- Establecer claramente y poner en práctica todas las directivas y procedimientos.
- Establecer programas de formación sobre la seguridad de la información, tanto para el personal de tecnología como para los usuarios finales.

- Monitoreo de red, registros y eventos del sistema.
- Gestión de parches de seguridad (Sistemas operativos, bases de datos, software)
- Aseguramiento de plataforma (configuraciones por defecto, hardening)
- Prevención de código malicioso.
- Sensibilización y entrenamiento de usuarios.

Acciones que cuenta el IDARTES

- Políticas de Seguridad de la Información http://comunicarte.idartes.gov.co/download/file/fid/2324
- Política de acceso a la red inalámbrica IDARTES http://comunicarte.idartes.gov.co/download/file/fid/3459
- Organización Interna Seguridad de la Información http://comunicarte.idartes.gov.co/download/file/fid/2214
- Identificación de activos de información de TI y metodología de activos de información http://comunicarte.idartes.gov.co/download/file/fid/2199
- Procedimiento de Gestión de Incidentes de Seguridad de la información http://comunicarte.idartes.gov.co/download/file/fid/2376
- Procedimiento Copia y Restauración de la Información http://comunicarte.idartes.gov.co/download/file/fid/2377

3.2 DETECCIÓN Y ANÁLISIS

Identificar las caracteristicas de un ataque, verificar que realmente ha sucedido y en el caso afirmativo, determinar su tipo y magnitud. No es fácil en todos los casos determinar con precisión si se ha producido o no un incidente de seguridad de la información y si es asi, identificar su tipo y evaluar a priori su peligrosidad.
La correcta detección de un incidente de seguridad se realiza mediante diferentes fuentes: IDS (Sistema de detección de intrusos), sistemas antivirus, caidas de servidores, reportes de usuarios, monitoreo, logs y alertas en sistemas de seguridad

3.2.1 Identificación de la gravedad del ataque

Para poder recuperarse de forma eficaz de un ataque, se debe determinar la gravedad de la situación de peligro que han sufrido los sistemas.
Debemos determinar:
• La naturaleza del ataque.
• El punto de origen.
• La intención del ataque. ¿Estaba el ataque dirigido especificamente a nuestra organización para conseguir información concreta o fue un ataque aleatorio?

3.2.2 Reporte de eventos e incidentes de seguridad de la información

La recepción de incidentes de seguridad a partir del personal de la entidad o de entes externos se realiza a través del correo soportesistemas@idartes.gov.co y como segunda opción vía telefónica, o personal a la oficina del área de sistemas
Para la correcta gestión de un incidente debemos registrar, al menos, los siguientes datos:

Figura 2. Formato reporte de incidentes de seguridad de la información

REPORTE DE EVENTOS/INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN	
Fecha del incidente: DD / MM / AAAA	**Hora:** HH.MM
DATOS DE LA PERSONA QUE REPORTA	
Nombres y apellidos:	**Dirección:**
Teléfono:	**Correo Electrónico:**
DESCRIPCIÓN DEL INCIDENTE	
Clase de incidente	
Código malicioso (Malware): ___ Robo de información: ___ Abuso/uso inadecuado de sistemas de información: ___ Borrado (compromiso) de información: ___	Acceso no autorizado: ___ Denegación de servicio (DoS): ___ Intrusiones: ___ Otro: ___
Qué ocurrió:	
Cómo ocurrió:	
Por qué ocurrió:	
Hardware/software involucrado en el incidente:	
Vulnerabilidad o amenaza identificada:	
EQUIPO DE RESPUESTA FRENTE A INCIDENCIAS DE SEGURIDAD INFORMATIVA (CSIRT)	
Responsable de atención el incidente:	

Individuos externos/entidades notificadas: CCP CAI VIRTUAL ___ COLCERT: ___**ccc** Otro (cual): _____
Acciones para resolver el incidente:
Acciones pendientes:
Observaciones:

Fuente: Autor

De igual manera se debe tener en cuenta los procedimientos y formatos otorgados por el CSIRT Gobierno a través del Ministerio TIC y Policía Nacional.

3.2.3 Clasificación de incidentes de seguridad

Los siguientes ataques que pueden ocasionar incidentes de seguridad se encuentran publicados en los ANS de la entidad y catalogados en la mesa de ayuda GLPI.

Tabla 1. Clasificación de incidentes de seguridad

CLASIFICACIÓN DE INCIDENTES DE SEGURIDAD		
CLASE DE INCIDENTE	**DESCRIPCIÓN**	**TIPO DE INCIDENTE**
Código malicioso (Malware)	Los códigos maliciosos identifican un programa o parte de éste insertado en otro programa, con la intención de modificar su comportamiento original.	virus, gusanos, troyanos, spyware, rootkit, ransomware (secuestro informático), códigos móviles y combinaciones de estos.
Robo de información	Ataques dirigidos a recabar información fundamental que permita avanzar en ataques más sofisticados, a través de ingeniería social o de identificación de vulnerabilidades.	- Robo de información digital (Carpetas, bases de datos) - Identificación de vulnerabilidades - (scanning) - Sniffing - Ingeniería social - Phishing
Abuso/uso inadecuado de sistemas de	Este tipo de incidentes ocurre cuando un usuario viola las políticas de seguridad del sistema de información de la organización. Ataques dirigidos	- Descargar e instalar herramientas para piratería informática.

información	a dañar la imagen de la organización o a utilizar sus medios electrónicos para otros usos ilícitos	- Usar el correo corporativo para correo basura o para la promoción de negocios personales; - Usar recursos corporativos para crear un sitio web no autorizado - Usar actividades entre colegas para adquirir o distribuir archivos piratas (música, video, software).
Borrado (compromiso) de información	Incidentes relacionados con el acceso y fuga (Confidencialidad), modificación o borrado (Integridad) de información no pública.	- Acceso no autorizado a información - Modificación y borrado no autorizada de información. - Publicación no autorizada de Información
Acceso no autorizado	Intentos reales no autorizados, para acceder o utilizar incorrectamente un sistema, servicio o red por parte de una persona, sistema o código malicioso	- Intentos por recuperar archivos de contraseñas - Ataques por desbordamiento de búfer para obtener acceso privilegiado a un objetivo - Aprovechamiento de las vulnerabilidades del protocolo para secuestrar o dirigir equivocadamente las conexiones de red legítimas - Intentos de elevar privilegios a recursos o información más allá de los que un usuario o administrador ya posee legítimamente. - Violaciones a las medidas de seguridad física
Denegación de servicio (DoS) y la denegación del servicio distribuido (DDoS) **(Disponibilidad)**	Permiten que un sistema, servicio o red dejen de operar a su capacidad prevista consumiendo sus recursos (Memoria RAM, CPU, Capacidad de almacenamiento y recursos de red). Estos tipos de ataques por lo general se realizan con frecuencia por medio de botnets, un grupo de robots de software (códigos maliciosos) que funcionan en forma autónoma y automática Los botnets pueden comunicarse con centenares o millones de computadores afectados.	- Robo, daño intencionado y destrucción de equipos - Daño accidental al hardware por incendio o daño por agua/inundación - Cambios en las condiciones ambientales por ejemplo las altas temperaturas - Sobrecarga y mal funcionamiento de los sistemas de información, software y hardware
Intrusiones	Ataques dirigidos a la explotación de	- Compromiso de cuenta de usuario

	vulnerabilidades de diseño, de operación o de configuración de diferentes tecnologías, al objeto de introducirse de forma fraudulenta en los sistemas de información y sitios web de la entidad.	- Defacement (desfiguración) - Cross-Site Scripting (XSS) - Cross-Site Request Forgery (CSRF) - Falsificación de petición entre sitios cruzados - Inyección SQL - Spear Phishing - Pharming - Ataque de fuerza bruta - Inyección de Ficheros Remota - Explotación de vulnerabilidad software - Explotación de vulnerabilidad hardware

Fuente: Autor

3.2.4 Priorización de los incidentes

Nivel de Prioridad: Depende del valor o importancia dentro de la entidad y del proceso que soporta el o los sistemas afectados.

Con el fin de permitir una atención adecuada a los incidentes (análisis, contención y erradicación) se debe determinar el nivel de prioridad del mismo, y de esta manera atenderlos adecuadamente según la necesidad.

Tabla 2. Niveles de Criticidad

Nivel Criticidad	Valor	Descripción
Inferior	1	Sistemas no críticos, como estaciones de trabajo de usuarios con funciones no críticas.
Bajo	2	Sistemas que apoyan a una sola dependencia o proceso de una entidad.
Medio	3	Sistemas que apoyan más de una dependencias o proceso de la entidad.
Alto	4	Sistemas pertenecientes al área de Tecnología y estaciones de trabajo de usuarios con funciones críticas.
Superior	5	Sistemas Críticos (de acuerdo al análisis de los activos de información de TI)

Fuente: GTC-ISO/ IEC 27035 – Guía Gestión de incidentes – MINTIC

Impacto Actual: Depende de la cantidad de daño que ha provocado el incidente en el momento de ser detectado.
Impacto Futuro: Depende de la cantidad de daño que pueda causar el incidente si no es contenido, ni erradicado.

Tabla 3. Niveles de Impacto

Nivel Impacto	Valor	Definición
Inferior	1	Impacto leve: Si el hecho llegara a presentarse, tendría consecuencias o efectos mínimos sobre la entidad y no se vería afectado en su continuidad de cualquier Sistema de información o estación de trabajo
Bajo	2	Impacto Bajo: Si el hecho llegara a presentarse, tendría bajo impacto o efecto sobre la entidad y se vería afectado en su continuidad de manera mínima de cualquier Sistema de información o estación de trabajo
Medio	3	Impacto Medio: Si el hecho llegara a presentarse, tendría medianas consecuencias o efectos sobre la entidad y se vería afectado en su continuidad de manera moderada de cualquier Sistema de información o estaciones de trabajo.
Alto	4	Impacto Alto: Si el hecho llegara a presentarse, tendría altas consecuencias o efectos sobre la entidad y se vería afectado en su continuidad de manera considerable interrumpiendo periódicamente los Sistemas de información o estaciones de trabajo.
Catastrófico	5	Impacto catastrófico: Si el hecho llegara a presentarse, tendría desastrosas consecuencias o efectos sobre la entidad y se vería afectado en su continuidad de manera total en los Sistemas de información o estaciones de trabajo.

3.3 CONTENER, ERRADICAR Y RECUPERAR

Con la contención permite proteger sistemas y redes limitando el daño, en esta fase se detección del incidente con el fin de que no se propague y pueda generar más daños a la información o a la infraestructura de tecnología y posteriormente erradicación del incidente o recuperación de los sistemas afectados.
Contención: busca la detección del incidente con el fin de que no se propague y pueda generar más daños a la información o a la arquitectura de TI.
Recuperar: Devolver los sistemas afectados por el incidente a su estado operativo. También contempla la eliminación de los componentes que han provocado el incidente igualmente se debe tener en cuenta lo establecido en el **PLAN DE CONTINGENCIAS DE TI.**

Tabla 4. Estrategia de contención, erradicación y recuperación

INCIDENTE	Ejemplos de incidentes	Nivel Criticidad	Nivel Impacto	Estrategia de contención	Estrategia de erradicación y recuperación.
Código malicioso (Malware)	virus, gusanos, troyanos, spyware, rootkit, ransomware (secuestro	Alto	Catastrófico	Desconexión de la red del equipo afectado.	Corrección de efectos producidos. Restauración de

	informático), códigos móviles y combinaciones de estos.				backups Reinstalación del equipo y recuperación de datos
Robo de información	- Robo de información digital (Carpetas, bases de datos) - Identificación de vulnerabilidades - (scanning) - Sniffing - Ingeniería social - Phishing	Superior	Catastrófico	Desconectar el recurso compartido.	Recuperación de datos a partir de copias de seguridad
Abuso/uso inadecuado de sistemas de información	- Descargar e instalar herramientas para piratería informática. - Usar el correo corporativo para correo basura o para la promoción de negocios personales; - Usar recursos corporativos para crear un sitio web no autorizado - Usar actividades entre compañeros para adquirir o distribuir archivos piratas (música, video, software).	Alto	Alto	Uso de políticas de seguridad de información.	Aplicar de nuevas reglas en firewalls.
Borrado (compromiso) de información	- Acceso no autorizado a información - Modificación y borrado no autorizada de información. - Publicación no autorizada de Información	Superior	Alto	Desconectar el recurso compartido. Suspender o eliminar la publicación no autorizada	Recuperación de datos

Acceso no autorizado	- Intentos por recuperar archivos de contraseñas - Ataques por desbordamiento de búfer para obtener acceso privilegiado a un objetivo - Aprovechamiento de las vulnerabilidades del protocolo para secuestrar o dirigir equivocadamente las conexiones de red legitimas - Intentos de elevar privilegios a recursos o información más allá de los que un usuario o administrador ya posee legítimamente. - Violaciones a las medidas de seguridad física	Alto	Alto	Apagado del sistema	Cambios de contraseñas. Aplicar de nuevas reglas en firewalls.
Denegación de servicio (DoS) y la denegación del servicio distribuido (DDoS) **(Disponibilidad)**	- Robo, daño intencionado y destrucción de equipos - Daño accidental al hardware por incendio o daño por agua/inundación - Cambios en las condiciones ambientales por ejemplo las altas temperaturas - Sobrecarga y mal funcionamiento de los sistemas de información, software y hardware	Superior	Catastrófico		Restitución del servicio caído
Intrusiones	- Compromiso de cuenta de usuario	Alto	Alto	Incorporación de reglas de filtrado en el firewall	La reinstalación de parches o la

	- Defacement (desfiguración) - Cross-Site Scripting (XSS) - Cross-Site Request Forgery (CSRF) - Falsificación de petición entre sitios - cruzados - Inyección SQL - Spear Phishing - Pharming - Ataque de fuerza bruta - Inyección de Ficheros Remota - Explotación de vulnerabilidad software - Explotación de vulnerabilidad hardware				aplicación de nuevas reglas en firewalls. Reparar el sitio web

Fuente: Autor

Recopilación y organización de pruebas del incidente

El equipo de respuesta de incidentes debe documentar, minuciosamente, todos los procesos al tratar con un incidente. Se debe incluir una descripción de la infracción y detalles de cada acción tomada (quién llevó a cabo la acción, cuándo lo hizo y por qué motivos), para tal caso se debe llevar al apartado de EVIDENCIA DIGITAL

3.4 POST INCIDENTE (LECCIONES APRENDIDAS)

Una de las fases más importantes de un plan de respuesta a incidentes de tecnología es aprender del incidente y la mejora continua. Por tal motivo se debe mantener documentación y/o registros que permita conocer exactamente lo que sucedió, en qué momento y cómo el personal gestionó el incidente. Una vez que se hayan finalizado las fases de documentación y recuperación, debemos revisar el proceso minuciosamente, determinar qué pasos se siguieron correctamente y qué errores se cometieron.

Las actividades en esta fase incluyen:
- Escribir el informe de incidente

- Analizar los problemas encontrados durante la respuesta a incidentes.
- Verificar las herramientas o recursos adicionales son necesarios para detectar, analizar y mitigar los incidentes en el futuro.
- Proponer mejoras basadas en los problemas encontrados
- Presentación del informe a las partes interesadas pertinentes

4. RECURSOS NECESARIO PARA ATENCION A INCIDENTES

Los miembros del equipo deben tener definidas claramente sus tareas para asegurar de que no quede ningún área de la respuesta sin cubrir.

Debemos asegurarnos de que contamos con los nombres y números de teléfono de contacto de las personas de la organización a las haya que avisar (incluidos los miembros del CSIRT) también necesitamos los detalles del proveedor de servicios de Internet (PSI) y las autoridades locales y nacionales.

4.1 Recurso Humano

Los actores que intervienen y conforman el proceso de atención de Incidentes

- Usuarios internos (Contratistas, funcionarios y visitantes)
- Líder de equipo
- Equipo de soporte técnico
- Administradores y/o ingenieros de la red y conectividad
- Administradores y/o ingenieros del sistema de información
- Administrador y/o ingenieros de infraestructura
- Área de mantenimiento e infraestructura.
- Personal seguridad de la información.
- Analista Forense

El equipo realizará las siguientes tareas:

- Supervisar los sistemas en busca de vulnerabilidades de seguridad.
- Servir como punto central de comunicación, tanto para recibir los informes de incidentes de seguridad como para difundir información esencial sobre los incidentes a las entidades correspondientes.
- Documentar y catalogar los incidentes de seguridad.
- Aumentar el nivel de conciencia y sensibilización con respecto a la seguridad dentro del IDARTES, para ayudar a evitar que se vuelva a suceder incidentes
- Posibilitar la auditoria de sistemas y redes mediante procesos como la evaluación de vulnerabilidades y

pruebas de penetración.

- Obtener más información sobre las nuevas vulnerabilidades y estrategias de ataque empleadas por los atacantes.
- Investigar acerca de nuevas revisiones de software.
- Analizar y desarrollar nuevas tecnologías para minimizar los riesgos y vulnerabilidades de seguridad.
- Perfeccionar y actualizar continuamente los sistemas y procedimientos actuales.

4.2 Recursos de comunicación

Información de Contacto: la lista de información de contacto de cada una de las personas que conforman el grupo de gestión de incidentes o quienes realicen sus funciones se encuentra establecida en el plan de gestión de incidentes.

Información de Escalamiento: para el escalamiento de incidentes se debe realizar de acuerdo a los procedimientos de Soporte Técnico y Gestión de Incidentes de Seguridad de la información y todo incidente de seguridad de la información centralizado a través del área de sistemas.

Para las acciones disciplinarias se escala a través de talento humano y el control disciplinario.

Política de Comunicación: La entidad a través de intranet http://comunicarte.idartes.gov.co y el correo electrónico de los usuarios se informará de los incidentes ocasionados de la entidad como medida de prevención.

Contacto Entidades externas:

Contacto con áreas interesadas o grupos de interés como primer canal de atención:

- CSIRT Gobierno.
- Cuando se tenga evidencia de un incidente informático, la entidad afectada se pondrá en contacto con el CAI Virtual de la Policía Nacional www.ccp.gov.co , Centro Cibernético Policial de la Policía Nacional al teléfono 4266900 ext.104092, para recibir asesoría del caso en particular y posterior judicialización.
- ColCERT Grupo de respuesta a emergencias cibernéticas de Colombia http://www.colcert.gov.co/?q=contenido/reportar-un-incidente, correos electrónicos: contacto@colcert.gov.co, malware@colcert.gov.co. o al Teléfono:(+571)2959897

4.3 Recursos técnicos

Para una correcta y eficiente gestión de incidentes la entidad debería tener en cuenta los siguientes elementos:

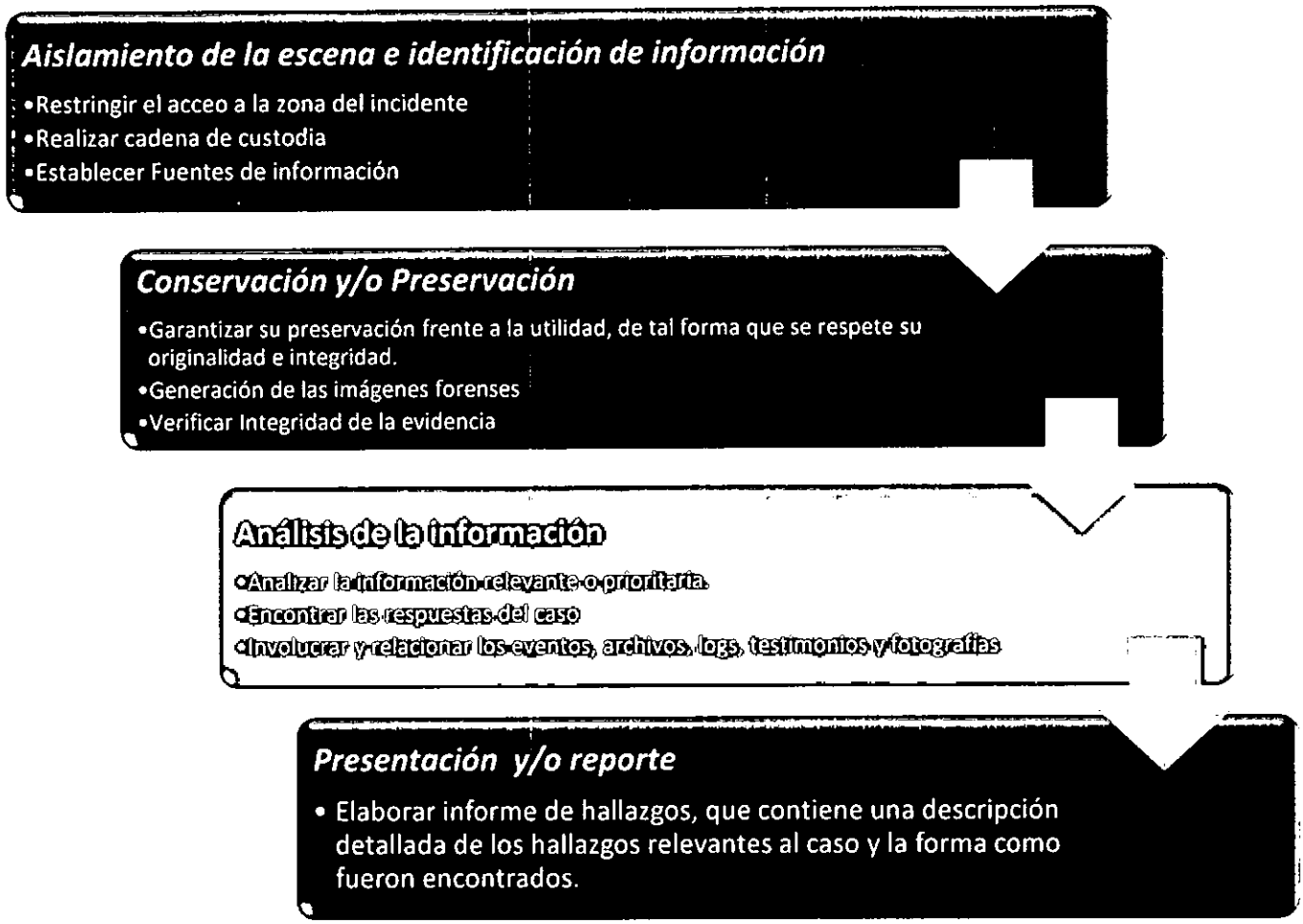
- Portátiles Forenses: facilitarles equipos portátiles reconfigurados con estas herramientas para asegurar que no se malgasta tiempo en la instalación y configuración de las herramientas, de modo que puedan responder a los incidentes
- Analizadores de protocolos.
- Software de adquisición.
- Software para recolección de evidencia.
- Kit de respuesta a incidentes.
- Software de análisis forense.
- Medios de almacenamiento
- Tener un listado de los puertos conocidos y de los puertos utilizados para realizar un ataque.
- Tener un diagrama de red para tener la ubicación rápida de los recursos existentes
- Una Linea – Base de Información de: Servidores (Nombre, IP, Aplicaciones, Parches, Usuarios Configurados, responsable de cambios). Esta información siempre debe estar actualizada para poder conocer el funcionamiento normal del mismo y realizar una identificación más acertada de un incidente.
- Se debe tener un análisis del comportamiento de red estándar en este es recomendable incluir: puertos utilizados por los protocolos de red, horarios de utilización, direcciones IP con que generan un mayor tráfico, direcciones IP que reciben mayor número de peticiones.

5. EVIDENCIA DIGITAL

Evidencia construida por campos magnéticos y pulsos electromagnéticos que pueden ser recolectados, almacenados, y analizados con herramientas especiales.
Características de la evidencia digital:

- **Duplicable y reemplazable:** duplicada y copiada de forma exacta como si fuera la original
- **Alterable:** se puede identificar si fue alterada
- **Borrable:** es posible en la mayoría de los casos recuperar la información
- **Volátil:** existen copias o información en otras partes del sistema

Figura 3. Etapas gestión de incidentes



Fuente: Autor – ISO 27037 Recopilación de Evidencias digital.

5.1 Aislamiento de la escena e identificación de información

Una vez el evento reportado se cataloga como un incidente de seguridad de la información, es necesario restringir el acceso a la zona donde se produjo el incidente para evitar cualquier tipo de alteración o contaminación a la evidencia

Dependiendo la rigurosidad del incidente y teniendo en cuenta que los procedimientos se deben ejecutar en la brevedad posible debe proceder el personal de la institución (preferiblemente un ingeniero forense o de seguridad

de la información) que esté en capacidad de describir detalladamente todos los procedimientos que realizó para aislar la escena y capturar evidencia en primera instancia. Si se tiene inconvenientes o dudas para realizar el procedimiento se pide acompañamiento al centro cibernético policial CCP CAI Virtual https://caivirtual.policia.gov.co/ , o al Grupo de Respuesta a Emergencias Cibernéticas de Colombia - colCERT.

Procedimiento por realizar para aislar la escena:

- Tomar fotografías del equipo antes de entrar en contacto.
- Se debe prevenir el acceso no autorizado de personal a la escena, estableciendo un perímetro de seguridad, para que nadie pueda acercarse.
- Identificar todos aquellos posibles elementos que sea susceptibles de almacenar (dispositivos que pueden almacenar datos electrónicamente.
- Si el equipo se encuentra encendido y se verifica que se está destruyendo la evidencia apagar inmediatamente, desconectando o retirando batería.
- Si el equipo se encuentra encendido, no se debe apagar, se debe sellar puertos USB, unidades, tomar fotografías de la pantalla, mantener el equipo encendido y evitar que se bloquee.
- Capturar la información volátil (RAM) y verificar cifrado del disco duro (si está cifrado se debe sacar imagen encendido), debe hacerse empleando las herramientas forenses necesarias.
- Si el equipo se encuentra apagado, no realizar el encendido, esto puede alterar la escena o borrar información que podría lograr obtenerse posteriormente.

Cadena de custodia

La cadena de custodia es un procedimiento que debe tenerse en cuenta desde el mismo instante que se decida realizar el proceso de evidencia forense se debe tener en cuenta:

- Hacer un inventario y descripción de los elementos
- Embalar las evidencias inventariadas en el contenedor, cerrado y etiquetado.
- Etiquetar con: Fecha y hora del hallazgo, numero de evidencia, número de registro (folio), dirección exacta del lugar de los hechos y descripción del material, observaciones, nombre completo del agente policial, perito o auxiliar responsable de la recolección y el embalaje.
- Una hoja de ruta, en donde se anotan los datos principales sobre descripción de la evidencia, fechas, horas, custodios, identificaciones, cargos y firmas de quien recibe y quien entrega
- Contar con los elementos necesarios para la recolección de información como estaciones forenses, dispositivos de backups, medios formateados y/o estériles, cámaras digitales, cinta y bolsas para evidencia, papel de burbuja, bolsas antiestáticas, cajas de cartón, rótulos o etiquetas.

Fuentes de información:

- Entrevistas administradoras de los sistemas de información y red, revisión topologia de red, entrevistas con el personal de la empresa que se hubiera tenido con el incidente, correos electrónicos, documentación referida del caso.
- Computadores de escritorio y portátiles
- Servidores (Web, DHCP, Email, Mensajería Instantánea, VoIP Servers, FTP o cualquier servicio de filesharing).
- Almacenamiento en red.
- Medios tanto internos como externos que contemplan: Dispositivos USB, Firewire, CD/DVD, PCMCIA, Discos Ópticos y Magnéticos, Discos Duros Extraíbles, Memorias SD y MicroSD.
- Dispositivos celulares, PDAs, Cámaras Digitales, Grabadoras de video y audio.

5.2 Conservación y/o Preservación

Una vez identificada la evidencia se debe garantizar su preservación frente a la utilidad, de tal forma que se respete su originalidad e integridad, garantizando a futuro que la evidencia sea admisible en un proceso judicial. De acuerdo con la Norma ISO 27037 la evidencia digital potencia debe ser tratada de acuerdo los siguientes principios: Reducir al mínimo la manipulación, documentar los cambios y las acciones adelantadas, cumplir con las normas locales de evidencia, no tomar acciones más allá de su competencia.
El procedimiento para preservar las evidencias digitales se debe tener en cuenta los siguientes pasos:

- Para el almacenamiento de las imágenes forenses se debe contar con medios estériles con una capacidad igual o superior a los discos identificados.
- Usar bloqueadores de escritura
- Generación de las imágenes forenses de tipo bit a bit mediante herramientas de extracción de imágenes como Linux dd o Encase Forensic Software, se sugiere sacar mínimo dos imágenes forenses.
- Verificar Integridad de la evidencia y cadena de custodia, para cada imagen suministrada se debe calcular su compendio criptográfico (SHA - 256), comparándolo luego con el de la fuente original. Si la comparación arroja un resultado negativo se debe rechazar la imagen proveída en el primer paso.
- Evitar una alteración no deseada en los medios
- No se trabaja sobre el bien informático (sobre escritura)
- En las zonas físicas se deben garantizar las medidas de seguridad necesarias para evitar alteración o intrusión a las evidencias halladas.

5.3 Análisis de la información

Una vez se ha definido los elementos materiales probatorios o evidencia, entramos a la fase de extraer, procesar e interpretar la información, en esta fase se determina toda una cadena de acontecimientos desde que se produjeron los hechos hasta su descubrimiento, dicho análisis puede involucrar y relacionar los eventos, archivos, logs, testimonios, fotografías, videos de vigilancia etc., para así llegar a alguna conclusión determinada.

Se debe tener en cuenta:

- Entorno de trabajo, a nivel físico un espacio que garantice la seguridad de los elementos probatorios recolectados.
- La evidencia se procesa para poder obtener información que entiendas los investigadores.
- Para interpretar se necesita conocimiento profundo como encajan las piezas.
- Obtención de la línea de tiempo de la evidencia.
- El análisis efectuado por el forense debe poder ser repetido.
- Aplicación de técnicas científicas a los medios duplicados, mediante las siguientes acciones:
    - Examinar los logs del sistema, fechas y horas del sistema, su respectiva zona horaria, los recursos y hardware instalado.
    - Usos de dispositivos USB
    - Determinar sistema operativo y las aplicaciones instaladas
    - Búsqueda de archivos específicos
    - Recuperación archivos eliminados
    - Identificación de información de tráfico de red
    - Identificación de archivos existentes
    - Identificación de archivos protegidos
    - Clasificación de archivos (modificados, sospechoso, extensión modificada)
    - Identificación de correos electrónicos
    - Acciones que el usuario realizo (historia, archivos abiertos)

5.4 Presentación de evidencias

Se elabora el informe de hallazgos, que contiene una descripción detallada de los hallazgos relevantes al caso y la forma como fueron encontrados.
En el reporte se debe contemplar los siguientes aspectos:

- El destino del informe, donde se relacione el cliente, autoridad o entidad solicitante.
- Descripción de los Procedimientos Técnicos empleados, entre ellos, la documentación fotográfica o videográfica, el proceso de extracción de la imagen forense y las actividades adelantadas.

- Cómo y por qué fueron utilizadas las diferentes herramientas y procedimientos para recolectar y analizar la información.
- Se debe tener en cuenta a la entidad o autoridad a presentar el informe, para lo cual se sugiere realizar dos informes, un informe técnico orientado al equipo técnico y/o ingenieros donde se contemple los equipos y herramientas forenses empleados, las técnicas y/o procedimientos, resultados y descripción de hallazgos. Por último, un informe gerencial y/o ejecutivo presentado en un lenguaje coloquial (no técnico) y de menor densidad que el informe técnico.
- Acciones por tomar (si es para remediar algún incidente o crimen), como por ejemplo mejorar determinados controles de seguridad.
- Presentación de resultados y su interpretación, las cuales señalan la información o datos obtenidos frente a la solicitud.

6. NORMATIVA

Guía para la Gestión y Clasificación de Incidentes de Seguridad de la Información (MSPI-MinTIC).

Guia Evidencia Digital (MSPI-MinTIC).

GTC-ISO/IEC 27035:2013 Gestión de incidentes de seguridad de la información

Manual de Manejo de Evidencias Digitales y Entornos Informáticos. Versión 2.0

Manual de procedimientos para Cadena De Custodia – FISCALIA General de la nación.

NTC-ISO-IEC27001:2013: Sistemas de Gestión de la Seguridad de la información.

NTC-ISO-IEC27037:2012: Guía para la identificación, recolección, adquisición y preservación de evidencias digitales.

Ley 527 de 1999: por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones.

Ley 1273 de 2009: de la protección de la información y de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones

Ley 1581 de 2012: Por la cual se dictan disposiciones generales para la protección de datos personales

7. DEFINICIONES

Cadena De Custodia: Su objetivo principal es demostrar 3 aspectos: El primero, que la información o evidencia está intacta al momento de presentarse, segundo, que la hora y fecha en la que se hace entrega al proveedor o las autoridades sea exacta y tercero, que no fue manipulada o alterada mientras se encontraba en custodia del proveedor.

Clave, Contraseña, Password: es la llave asignada por cada usuario para acceder a sus aplicaciones, la cual es personal e intransferible.

CSIRT: (Computer Security Incident Response Team), Equipo de Respuesta frente a Incidencias de Seguridad Informática.

CTSI: Comité Técnico de Seguridad de la Información

Evento de seguridad de la información: Presencia identificada de una condición, alerta o notificacion de un sistema, servicio o red, que indica una posible violación de la política de seguridad de la información o la falla de las salvaguardas o una situación desconocida previamente que puede ser pertinente para la seguridad.

Evidencia: Todo aquel elemento que proporcione información que conduzca a alguna conclusión o hallazgo relacionado con el hecho que se investiga.

Evidencia digital: Evidencia almacenada en soportes digitales.

Evidencias volátiles: Aquellas que desaparecen en ausencia de alimentación eléctrica.

GLPI: Herramienta que gestiona las incidencias o solicitudes de soporte de los usuarios de la entidad. Su sigla, traducidas de francés a español, significan: Gestión Libre del Parque Informático.

Incidente de seguridad de la información: Un evento o serie de eventos de Seguridad de la Información no deseados o inesperados, que tienen una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información.

Informática Forense: Aplicación de la ciencia para la identificación, recolección, examen y análisis de los datos, preservando correctamente su integridad, llevando a cabo a su vez una estricta cadena de custodia de la información.

Información Volátil: Datos de un determinado sistema que se pierden una vez dicho sistema es reiniciado o apagado

MINTIC: Ministerio de Tecnología de Información y las Comunicaciones

MSPI:.Modelo de Seguridad y Privacidad de la información

Plataforma tecnológica: Un conjunto de estándares, herramientas de hardware y software que apoyan el desarrollo de los procesos administrativos y misionales de la entidad.

Seguridad de la información: Preservación de la confidencialidad, integridad y disponibilidad de la información adicionalmente pueden involucrarse otras propiedades, tales como: autenticidad, responsabilidad, no repudio y confiabilidad.

TICS: Tecnologías de la Información y las Comunicaciones.

(Fuente ISO 27000, Guía Evidencia digital)